一种基于双重 KGC 的无证书短签名方案 *

左黎明 [a,b]，张梦丽 [a,b]，胡凯雨 [a,b]，易传佳 [a,b]

(华东交通大学 a. 理学院; b.系统工程与密码学研究所, 南昌 330013)

摘　要: 为了解决无证书短签名方案中单 KGC 权力过于集中的问题,提出一种基于双重 KGC 的无证书短签名方案,其中双重 KGC 之间相互制约,有效地减少了单 KGC 主密钥泄露和被恶意操控带来的危害。随后在随机预言机模型、k-CAA 和 Inv-CDH 问题困难性假设下，证明了签名方案在适应性选择消息攻击下是存在性不可伪造的。最后与其他无证书数字签名方案进行了比较，并用 C 语言实现了该方案.实验结果和分析表明该方案计算量较低，运行效率和安全性较高。

关键词: 无证书；双重 KGC；短签名；可证明安全；随机预言机模型

中图分类号: TP309.7　　doi: 10.19734/j.issn.1001-3695.2018.10.0828

Certificateless short signature scheme with double KGC

Zuo Liming[a,b], Zhang Mengli[a,b], Hu Kaiyu[a,b], Yi Chuanjia[a,b]

(a. *School of Science*, *b. SEC Institute*, *East China Jiaotong University*, *Nanchang* 330013, *China*)

Abstract: In order to solve the problem that the power of the single KGC in certificateless short signature is too concentrated, this paper proposed a certificateless short signature scheme with double KGC, in which double KGC was restricted by each other. So it can effectively reduce the harm of the single KGC's main key leakage and malicious manipulation. Then, under the random oracle model, the difficult problem of k-CAA and Inv-CDH, it proved that the signature scheme was existentially unforgeable under adaptive chosen message attack. Finally, it compared the signature scheme with other certificateless schemes, and implemented the signature scheme in C language. The experimental results and analysis show that the scheme has lower computational cost, higher operating efficiency and security.

Key words: certificateless; double kgc; short signature; provably secure; random oracle model

0　引言

为了解决传统公钥密码体制中用户公钥证书管理和证书传递耗时的问题，Shamir[1]于 1984 年提出了基于身份的密码体制，其中所有用户的私钥由一个可信的第三方私钥生成器 *(private key generator ,PKG)*生成，因此恶意的 *PKG* 可以冒充用户生成签名或者解密发给用户的密文，这样就存在一个密钥托管问题。为了解决基于身份的密码体制的密钥托管问题，2003 年，Al-Riyami 和 Paterson[2]提出了一个无证书的公钥密码体制，在无证书公钥密码体制中，用户私钥由密钥生成中心*(key generation centre, KGC)*与用户共同产生，这样既解决了基于身份的密码体制中的密钥托管问题，同时也消除了传统密码体制中证书的存储和管理问题。随后，许多无证书数字签名方案相继被提出。2012 年，冯蕾等人[3]在标准模型下提出了一个高效的无证书多重签名方案。2016 年，Islam 等人[4]基于双线性对构建了一个无证书数字签名方案。2017，Gao 等人[5]基于 *CDH(computational Diffie-Hellman)*问题提出了无泄露的无证书数字签名方案。

在无证书密码系统中，有两种类型攻击者[6] A_1 和 A_2，一种是不诚实的用户 A_1，它不知道系统主密钥及用户部分私钥，但可以代替用户的公钥；另一种是恶意的 *KGC* A_2，它掌握系统主密钥和用户部分私钥，但不能替换用户的公钥。

目前已有的基于单 *KGC* 的无证书签名方案，部分不能抵抗恶意 *KGC* 攻击。2017 年，张永洁等人[7]分析了文献[8~10]提出的无证书聚合签名方案的安全性，指出这三个方案存在恶意 *KGC* 攻击，并分别构造了攻击算法，实现了伪造攻击。同年，葛丽霞等人[11]分析了刘晓红和张建中提出的一个无证书代理签名方案[12]，发现其不能抵抗恶意 *KGC* 攻击。

因此可见，单个 *KGC* 的无证书签名方案由于 *KGC* 权力过大，恶意 *KGC* 可以掌握系统主密钥和用户的部分私钥，从而可以伪造签名，会对系统产生一定危害。为解决单 *KGC* 权力过于集中的问题，本文提出了一种在随机预言机模型下可证安全的基于双重 *KGC* 的无证书短签名方案，相比于其他基于单 *KGC* 无证书签名方案，一方面，双重 *KGC* 之间可以相互制衡，具有分权的效果，使得针对 *KGC* 的相关攻击的成功概率减少，从而可以降低对系统的危害，另一方面，结合了短签名[13]的优势，增强了本文方案的实用性。

1　基础知识

1.1　双线性映射

双线性对[14,15](*Bilinear Pairings*)：设 G_1 为 q 阶加法循环群，G_2 为 q 阶乘法循环群，P 为 G_1 的生成元，称映射 $e: G_1 \times G_1 \rightarrow G_2$ 为双线对，如果 e 满足以下三条性质：

a)双线性。对任意 $m, n \in Z_q^*$，有 $e(mP, nP) = e(P, P)^{mn}$。

b)非退化性。$e(P, P) \neq 1$。

c)可计算性。假设 $m, n \in Z_q^*$，则存在多项式时间算法计算

收稿日期: 2018-10-08; **修回日期:** 2018-12-26　**基金项目:** 国家自然科学基金资助项目(11761033)；江西省教育厅科技项目(GJJ161417, GJJ170386)

作者简介: 左黎明（1981-），男，江西鹰潭人，副教授，硕士，主要研究方向为信息安全，非线性系统 (limingzuo@126.com)；张梦丽（1992-），女，安徽亳州人，硕士研究生，主要研究方向为信息安全；胡凯雨（1995-），男，江西抚州人，硕士研究生，主要研究方向为信息安全；易传佳（1995-），男，江西宜春人，硕士研究生，主要研究方向为信息安全.

$e(mP,nP)$ 。

1.2　困难问题的假设

定义 1　$k-CAA$ 问题。对某一个整数 k 和 $s\in Z_q^*$ (s 是未知的随机数)，$P\in G_1$，给定 $\{e_1,e_2,\cdots,e_k\}\in Z_q^*$，$P,sP$ 和 $\left\{\frac{1}{s+e_1}P,\frac{1}{s+e_2}P,\cdots,\frac{1}{s+e_k}P\right\}$，计算 $(c,\frac{1}{s+c}P)$，其中 $c\in Z_q^*$，且 $c\notin\{e_1,e_2,\cdots,e_k\}$ 。

定义 2　逆 *CDH* 问题 (*inverse computational Diffie-Hellman problem*，*Inv-CDH*)。给定 $P\in G_1$，$aP\in G_1$ ($a\in Z_q^*$ 是未知的)，计算 $a^{-1}P$ 。

1.3　基于双重 KGC 的无证书数字签名定义

一个基于双重 *KGC* 的无证书数字签名方案由 7 个算法组成，具体如图 1 所示。

1.系统建立(*Setup*)：输入安全参数*L*,KGC_A运行算法,返回KGC_A系统主密钥x_A, KGC_B运行算法返回KGC_B系统主密钥x_B和系统公共参数*params*.

2.部分私钥提取(Extract-Partial-Private-Key)：输入*params*,KGC_A系统主密钥x_A,和身份*ID*, KGC_A运行该算法并输出KGC_A部分私钥d_A . 输入*params*,KGC_B系统主密钥x_B,和KGC_A部分私钥d_A，KGC_B运行该算法并输出部分私钥d_{ID},并通过安全信道发给相应的用户.

3.秘密值建立(*Set-Secret-Value*)：输入*params*和用户的身份*ID*,输出用户的秘密值x_{ID},该算法由系统中的每个用户来执行.秘密值空间是由系统公共参数*params*和用户的身份*ID*决定的.

4.私钥建立(*Set-Private-Key*)：输入*params*,用户的部分私钥d_{ID}和他的秘密值,输出私钥sk_{ID},该算法由系统中每个用户来执行.

5.公钥建立(*Set-Public-Key*)：输入*params*和用户的秘密值x_{ID},输出用户的公钥pk_{ID}.该算法由系统用户执行,且执行完该算法后公开公钥.公钥空间是由系统公共参数*params*和用户的身份信息*ID*共同定义的.

6.签名(*CL-Sign*)：输入*params*,待签名消息*m*,用户的身份*ID*,公钥pk_{ID}以及私钥sk_{ID},该算法输出签名*S*.

7.验证(CL-Verify)：这是一个确定的签名验证算法.输入*params*,签名人的身份*ID*,公钥pk_{ID},消息*m*以及签名*S*,返回"1"说明该签名有效,否则返回"0",说明该签名无效.

图 1　基于双重 KGC 的无证书数字签名定义

Fig. 1　Certificateless digital signature definition

1.4　基于双重 KGC 的无证书数字签名的安全模型

在无证书密码系统中，存在两种类型的攻击。一方面，因为用户公钥没有得到认证，所以敌手有权利用自己选择的不合法公钥替换用户的公钥，但不知道系统主密钥及用户的部分私钥，即存在用户公钥替换攻击；另一方面，由于 *KGC* 知道系统主密钥，从而可以计算出用户部分私钥，但是不能替换用户公钥，即存在恶意但被动的 *KGC* 攻击。因此，一个安全的无证书密码方案应该至少抵抗上述两种攻击。

本文基于上述传统单 *KGC* 无证书攻击类型，结合双重 *KGC* 的特点，详细给出了针对于本文方案具备不同能力的两种敌手，一种是不诚实的用户，记为 A_1，另一种是恶意但被动的 *KGC*，记为 A_2 。 这里将本文方案里的双重 *KGC* 记为 KGC_A 和 KGC_B 。

类型 *I* 的敌手 A_1 。至多知道一个 *KGC* 系统主密钥， 但不知道用户的部分私钥，并且能替换用户的公钥。

类型 *II* 的敌手 A_2 。掌握 KGC_A 和 KGC_B 系统主密钥，知道用户的部分私钥，但它不能替换用户的公钥。

定义 3　一个无证书数字签名方案在适应性选择消息攻击下是存在性不可伪造的，如果敌手 A_1，A_2 在以下两个游戏中获胜的概率是可以忽略的。

游戏 1

挑战者 *C* 和类型 *I* 的敌手 A_1 交互如图 2 所示。最后 A_1 输出一个挑战身份 ID^* 和公钥 pk_{ID^*} 的消息/签名对 (m^*,S^*) 。如果 $Verify(params,ID^*,m^*,pk_{ID^*},S^*)=1$ 和下面的条件成立，则 A_1 获胜。

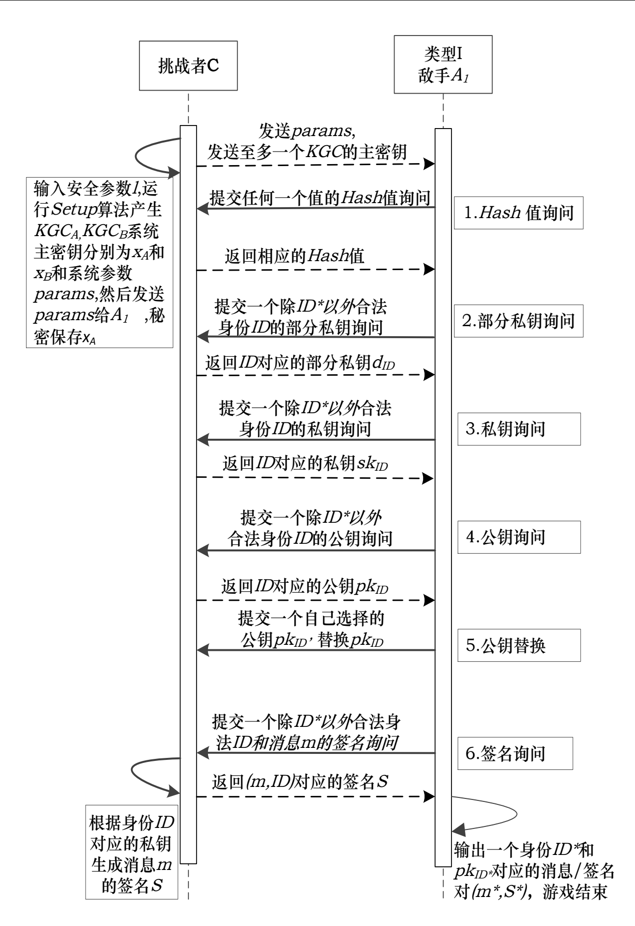


图 2　挑战者 C 与类型 I 敌手游戏过程

Fig. 2　Game process between Challenger C an d adversary of type I

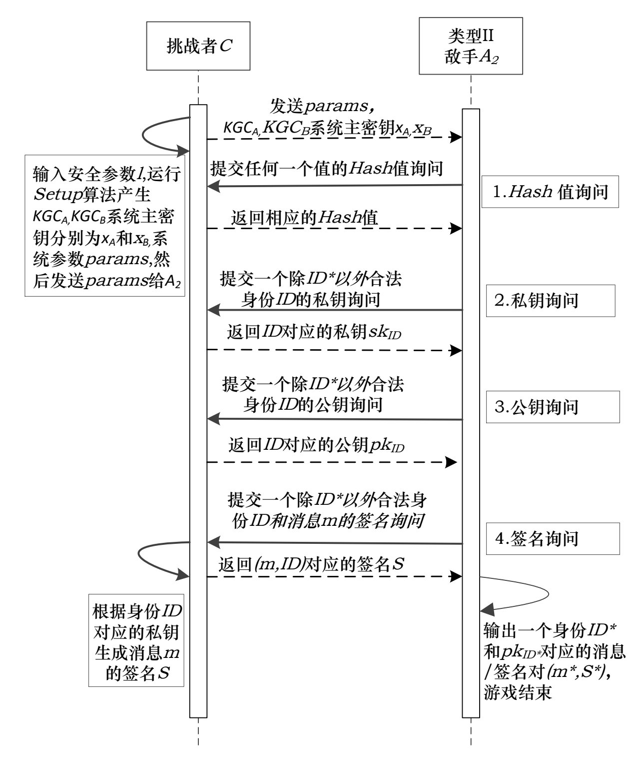


图 3　挑战者 C 与类型 II 敌手游戏过程

Fig. 3　Game process between Challenger C and adversary of type II

a) ID^* 从来没有被提交给私钥提取预言机；

b) ID^* 从来没有既被提交给替换公钥预言机又时提交给部分私钥提取预言机；

c) (m^*,S^*,ID^*,pk_{ID^*}) 不是由签名预言机得到的。

游戏 2

挑战者 C 和类型 II 的敌手 A_2 交互如图 3 所示。最后 A_2 输出一个挑战身份 ID^* 和公钥 pk_{ID^*} 的消息/签名对 (m^*,S^*) 。$Verify(params,ID^*,m^*,pk_{ID^*},S^*)=1$ 和下面的条件成立，则 A_2 获胜。

a) ID^* 从来没有被提交给私钥提取预言机；

b) (m^*,S^*,ID^*,pk_{ID^*}) 不是由签名预言机得到的。

2　基于双重 KGC 的无证书短签名方案

2.1　方案构造

a)系统建立。给定安全参数 l ，G_1 和 G_2 分别是加法循环群和乘法循环群，P 是 G_1 的生成元，G_1 的阶 q 。双线性对 $e:G_1\times G_1\to G_2$ ，选择两个抗碰撞的 Hash 函数：$H_1:\{0,1\}^*\to Z_q^*$ ，$H_2:\{0,1\}^*\times G_1\to Z_q^*$ 。KGC_A 选取一个秘密值 $x_A\in Z_q^*$ 作为 KGC_A 系统的私钥，计算 $y_A=x_AP\in G_1$ 作为 KGC_A 系统的公钥并公布，然后秘密保存 x_A 。KGC_B 选取一个秘密值 $x_B\in Z_q^*$ 作为 KGC_B 系统的私钥，计算 $y_B=x_BP\in G_1$ 作为 KGC_B 系统的公钥，并计算 $T=x_By_A=x_Ax_BP$ 作为联合公钥公布，然后秘密保存 x_B 。任何人都可以通过 $e(T,P)=e(y_A,y_B)$ 来验证 T 的有效性。KGC_A 和 KGC_B 公布联合系统参数 $params=\{G_1,G_2,e,q,P,H_1,H_2,y_A,y_B,T\}$ 。

b)部分私钥提取。给定身份 $ID\in\{0,1\}^*$ ，KGC_A 计算 $Q_{ID}=H_1(ID)$ ，$d_A=\frac{1}{x_A+Q_{ID}}P$ ，将 d_A 通过安全信道发送给 KGC_B 。KGC_B 首先验证 d_A 的有效性通过下面的等式成立：$e(d_A,y_A+Q_{ID}P)=e(P,P)$ 。验证成功后，计算 $Q_{ID}=H_1(ID)$ ，$d_{ID}=\frac{1}{x_B+Q_{ID}}d_A$ ，然后通过安全信道发送部分私钥 d_{ID} 给身份为 ID 的用户。

c)秘密值建立。用户 ID 随机挑选 $x_{ID}\in Z_q^*$ 作为自己的秘密值。

d)私钥建立。用户根据部分私钥 d_{ID} 和他的秘密值 x_{ID} ，输出数据 (d_{ID},x_{ID}) 作为该用户的私钥。

e)公钥建立。用户计算 $Q_{ID}=H_1(ID)$ ，$R=T+Q_{ID}y_A+Q_{ID}y_B+Q_{ID}^2P$ ，产生该用户的公钥为 $pk_{ID}=x_{ID}R$ 。

f)签名。身份为 ID 的用户对消息 $m\in\{0,1\}^*$ 签名如下：

(a)令 $h=H_2(m,pk_{ID})$ ；

(b)计算 $S=\frac{1}{h+x_{ID}}d_{ID}$ 。

则 S 就是身份为 ID 的用户对消息 m 的签名。

g)验证。给定消息/签名对 (m,S) ，验证者计算如下：

(a)令 $h=H_2(m,pk_{ID})$ ；

(b)接受该签名并返回 a）当且仅当以下等式成立：$e(S,hR+pk_{ID})=e(P,P)$ 。

签名等式的正确性证明如下：

$$e(S,hR+pk_{ID})=e(\frac{1}{h+x_{ID}}\cdot d_{ID},hR+pk_{ID})$$

$$=e(\frac{1}{h+x_{ID}}\cdot\frac{1}{x_B+Q_{ID}}\cdot\frac{1}{x_A+Q_{ID}}P,hR+pk_{ID})$$

$$=e(\frac{1}{h+x_{ID}}\cdot\frac{1}{x_Ax_B+x_AQ_{ID}+x_BQ_{ID}+Q_{ID}^2}P,hR+pk_{ID})$$

$$=e(\frac{1}{h+x_{ID}}\cdot\frac{1}{x_Ax_B+x_AQ_{ID}+x_BQ_{ID}+Q_{ID}^2}P,hR+x_{ID}R)$$

$$=e(\frac{1}{h+x_{ID}}\cdot\frac{1}{x_Ax_B+x_AQ_{ID}+x_BQ_{ID}+Q_{ID}^2}P,(h+x_{ID})R)$$

$$=e(\frac{1}{h+x_{ID}}\cdot\frac{1}{x_Ax_B+x_AQ_{ID}+x_BQ_{ID}+Q_{ID}^2}P,(h+x_{ID})\cdot(x_Ax_BP+Q_{ID}y_A+Q_{ID}y_B+Q_{ID}^2P))=e(P,P)$$

2.2　安全性分析

设单 KGC 密钥泄露的概率为 p ，那么本文所构造的双重 KGC 密钥泄露的概率为 p^2，所以如果基于单 KGC 是安全的，那么基于双重 KGC 也是安全的。

定理 1　在随机预言机模型中，在 q_E-CAA 及 $Inv-CDH$ 难题假设下，本文提出的基于双重 KGC 的无证书短签名方案在适应性选择消息攻击下是存在性不可伪造的。

定理 1 可由下面的引理 1~3 推导出。

引理 1　针对敌手 I 类型，假定存在一个适应性选择消息和签名攻击算法 A_1 以在概率多项式时间 t 内以不可忽略的优势 ε 攻破了本方案，不妨设 A_1 不知道 KGC_A 系统主密钥，但是知道 KGC_B 系统主密钥，并记 q_{H_i} ，q_E ，q_E' ，q_{pk} ，q_s 分别为 A_1 进行 $H_i(i=1,2)$ 询问、部分私钥提取询问、私钥提取询问、公钥询问和签名询问的次数，t_{Hi} ，t_E ，$t_{E'}$ ，t_{pk} ，t_s 分别表示一次 H_i 预言机询问、一次部分私钥提取预言机、一次私钥提取询问、一次公钥询问、一次签名询问所需时间，则存在一个 (t',ε') 算法 C ，在时间 $t'<t+(q_Et_E+q_{E'}t_{E'}+q_{pk}t_{pk}+q_St_S)+2(q_{H_1}t_{H_1}+q_{H_2}t_{H_2})$ 内以 $\varepsilon'\ge(\varepsilon-\frac{1}{2^k})(\frac{q_E}{q_{H_1}})^{q_E+q_E'+q_s}(\frac{q_{H_1}-q_E}{q_{H_1}})$ 优势解决 q_E-CAA 问题。

证明　给定算法 C 一个 q_E-CAA 问题的实例：公开 $P,y_A=x_AP\in G_1$ ，$,e_1,e_2,\cdots,e_{q_E}\in Z_q^*$ 和 $\frac{1}{x_A+e_1}P,\frac{1}{x_A+e_2}P,\cdots,\frac{1}{x_A+e_{q_E}}$（ x_A 是未知的），C 的目标是调用 A_1 为子程序，最后输出 q_E-CAA 问题的一个解 $(Q^*,\frac{1}{x_A+Q^*}P)$ ，其中 $Q^*\notin\{e_1,e_2,\cdots,e_{q_E}\}$ 。

在游戏中假定对任意用户身份 ID ，签名攻击算法 A_1 在进行部分私钥提取询问，私钥提取询问，公钥替换，签名询问以及输出签名之前都询问过关于用户身份 ID 的 H_1 和 H_2 预言机。

C 运行 KGC_A 系统建立算法，令 $y_A=x_AP$ 作为 KGC_A 系统的公钥(这里 x_A 充当的是 KGC_A 系统主密钥，x_A 对 C 是未知的)。

C 运行 KGC_B 系统建立算法，选择 $x_B\in Z_q^*$ 充当 KGC_B 系统主密钥，计算 $y_B=x_BP$ 作为 KGC_B ，系统的公钥，$T=x_By_A=x_Ax_BP$ 作为系统联合公钥(x_B 对是已知的)，发送系统联合参数 $params=\{P,H_1,H_2,y_A,y_B,T\}$ 和 KGC_B 系统主密钥 x_B 给 A_1 。则攻击算法 A_1 向挑战者 C 适应性执行下面询问：

a) H_1 询问：C 维护一个列表 H_1^{list} ，该列表由表项 (ID_i,Q_i) 组成的，构造如下：准备了 q_{H_1} 个应答 $Q_1,Q_2,\cdots,Q_{q_{H_1}}$ ，其中将数据 $e_1,e_2,\cdots,e_{q_E}$ 随机分布在集合中。当 A_1 进行关于身份 ID_i 的 H_1 询问，C 执行如下操作：

(a)如果 $ID_i=ID^*$ ，C 从列表中挑选一个 $Q^*\notin\{e_1,e_2,\cdots,e_{q_E}\}$ 返回给 A_1 。

(b)否则，C 从集合 $\{e_1,e_2,\cdots,e_{q_E}\}$ 中随机挑选一个值 e_i ，并令 $H_1(ID_i)=e_i$ ，返回 $Q_i=e_i$ 给 A_1 。

b)部分私钥提取询问。C 维护一个列表 E^{list} ，该列表由表项 (ID_i,Q_i,d_{ID_i}) 组成。当 A_1 进行关于身份 ID_i 的部分私钥时，C 从 H_1^{list} 中恢复 (ID_i,Q_i) ，然后执行如下操作：

(a)如果 $Q_i \in \{e_1, e_2, \cdots, e_{q_E}\}$，则令 $d_{ID_i} = \frac{1}{x_B + Q_i}\frac{P}{x_A + Q_i}$（不妨设 $Q_i = e_j$），然后将 d_{ID_i} 返回给 A_1 并增加记录 (ID_i, Q_i, d_{ID_i}) 到列表 E^{list}。

(b)否则 C 停止模拟并输出"FAILURE"(该事件发生用 E_1 表示)。

c)公钥询问。C 维护一个列表 pk^{list}，该列表由表项 $(ID_i, Q_i, pk_{ID_i}, r_i)$ 组成，该表初始化为空。当 A_1 进行关于身份 ID_i 的公钥询问时，C 检查列表中是否存在对应的值。如果存在，则输出对应的值。否则，C 从列表 $H_1^{list}:(ID_i, Q_i)$ 恢复出 Q_i，然后挑选一个随机数 $r_i \in Z_q^*$，计算 $pk_{ID_i} = r_i(T + Q_i y_A + Q_i y_B + Q_i^2 P)$，并返回公钥 pk_{ID_i} 给 A_1。然后增加记录 $(ID_i, Q_i, pk_{ID_i}, r_i)$ 到列表 pk^{list}。

d)私钥提取询问。当 A_1 进行关于身份 ID_i 的私钥提取询问时，C 首先从 H_1^{list} 列表中恢复出 Q_i，然后执行如下操作：

(a)如果 $Q_i \in \{e_1, e_2, \cdots, e_{q_E}\}$，从列表 E^{list} 和列表 pk^{list} 中恢复出相应的记录 (ID_i, Q_i, d_{ID_i}) 和记录 $(ID_i, Q_i, pk_{ID_i}, r_i)$，$C$ 令 $sk_{ID_i} = (d_{ID_i}, r_i)$ 并将 sk_{ID_i} 作为对应私钥返回给 A_1。

(b)否则，C 停止协议并输出"FAILURE"(该情况用 E_2 表示)。

e)公钥替换。A_1 输入 (ID_i, pk'_{ID_i})，C 修改列表 pk^{list} 中的记录 $(ID_i, Q_i, pk_{ID_i}, r_i)$ 为 $(ID_i, Q_i, pk'_{ID_i}, r_i)$，将用户 ID_i 的公钥 pk_{ID_i} 替换为 pk'_{ID_i}。

r) H_2 询问。C 维护一个列表 H_2^{list}，该列表由表项 $(ID_i, m_i, Q_i, pk_{ID_i}, h_i)$ 组成。当 A_1 进行关于 (ID_i, m_i) 的 H_2 询问时，C 随机选择 $h_i \in Z_q^*$，令 $h_i = H_2(m_i, pk_{ID_i})$ 并返回给 A_1，然后增加记录 $(ID_i, m_i, Q_i, pk_{ID_i}, h_i)$ 到 H_2^{list}。

g)签名询问。当 A_1 进行关于 (ID_i, m_i) 的签名询问时，C 首先从 H_1^{list} 中恢复 (ID_i, Q_i)，然后执行如下操作：

(a)如果 $Q_i \in \{e_1, e_2, \cdots, e_{q_E}\}$，$C$ 从列表 E^{list} 提取记录 (ID_i, Q_i, d_{ID_i})，从 pk^{list} 中提取记录 $(ID_i, Q_i, pk_{ID_i}, r_i)$，从列表 H_2^{list} 中提取记录 $(ID_i, m_i, Q_i, pk_{ID_i}, h_i)$，计算 $S_i = \frac{1}{r_i + h_i} d_{ID_i} = \frac{P}{(r_i + h_i)(x_A + Q_i)(x_B + Q_i)}$。

(b)否则，停止协议，输出"FAILURE"(该情况用 E_3 表示)。C 输出签名 S_i。

最后，A_1 停止训练并输出一个挑战身份 ID^* 的消息/签名对 (m^*, S^*)，ID^* 对应的公钥为 pk_{ID^*}，且满足等式 $Verify(m^*, ID^*, pk_{ID^*}, S^*) = 1$。$C$ 从列表 pk^{list} 提取相应的记录 $(ID^*, Q^*, pk_{ID^*}, r^*)$，从列表 H_2^{list} 提取记录 $(ID^*, m^*, Q^*, pk_{ID^*}, h^*)$，然后执行如下操作：

(a)如果 $Q^* \in \{e_1, e_2, \cdots, e_{q_E}\}$，$C$ 输出"FAILURE"并停止该协议(该事件用 E_4 表示)。

(b 否则，就有下面的等式成立：

$$e(S^*, h^*(T + Q^* y_A + Q^* y_B + Q^{*2}P) + pk_{ID^*}) = e(P, P)$$

即

$$\begin{aligned} & e(S^*, (h^* + r^*)(T + Q^* y_A + Q^* y_B + Q^{*2}P) \\ & = e(S^*(h^* + r^*)(x_A + Q^*)(x_B + Q^*), P) \\ & = e(P, P) \end{aligned}$$

所以 C 可以成功地计算出 $\frac{1}{(x_A + Q^*)}P = (h^* + r^*)(x_B + Q^*)S^*$。

C 输出数组 $(Q^*, \frac{1}{(x_A + Q^*)}P)$，$Q^* \notin \{e_1, e_2, \cdots, e_{q_E}\}$ 作为问题的解，从而 C 解决了 $q_E - CAA$ 问题。

下面分析 C 在这个游戏中获胜的优势：

a) A_1 的 H_1 和 H_2 的询问的应答是均匀分布的，与现实不可区分。

b)部分私钥提取询问，私钥提取询问和签名询问能够顺利的进行不停止，即事件 E_1，E_2，E_3 都不发生。

c)果事件 E_1，E_2，E_3 和 E_4 都不发生时，则 C 能解决 $q_E - CAA$ 问题的一个实例。则可得事件 E_1，E_2，E_3 和 E_4 都不发生的概率满足：

$$\Pr(\neg E_1 \wedge \neg E_2 \wedge \neg E_3 \wedge \neg E_4) \ge (\frac{q_E}{q_{H_1}})^{q_E + q'_E + q_s}(\frac{q_{H_1} - q_E}{q_{H_1}})$$

但是当 A_1 没有询问 H_2 而伪造了一个有效的签名时，这种模拟是存在漏洞的，考虑到预言机输出满足均匀分布，该事件发生的概率为 $\frac{1}{2^k}$，所以 C 在该游戏中的优势为 $\varepsilon' \ge (\varepsilon - \frac{1}{2^k})(\frac{q_E}{q_{H_1}})^{q_E + q'_E + q_s}(\frac{q_{H_1} - q_E}{q_{H_1}})$，运行时间满足 $t' < t + (q_E t_E + q'_E t_{E'} + q_{pk} t_{pk} + q_S t_S) + 2(q_{H_1} t_{H_1} + q_{H_2} t_{H_2})$。

引理 2 对敌手 I 类型，假定存在一个适应性选择消息和签名攻击算法 A_1 以在概率多项式时间 t 内以不可忽略的优势 ε 攻破了本方案，不妨设 A_1 既不知道 KGC_A 系统主密钥，也不知道 KGC_B 系统主密钥，并记 q_{H_i}，q_E，q'_E，q_{pk}，q_s 分别为 A_1 进行 $H_i(i = 1,2)$ 询问、部分私钥提取询问、私钥提取询问、公钥询问和签名询问的次数，t_{Hi}，t_E，$t_{E'}$，t_{pk}，t_s 分别表示一次 H_i 预言机询问、一次部分私钥提取预言机、一次私钥提取询问、一次公钥询问、一次签名询问所需时间，则存在一个 (t', ε') 算法 C，在时间 $t' < t + (q_E t_E + q_{E'} t_{E'} + q_{pk} t_{pk} + q_S t_S) + 2(q_{H_1} t_{H_1} + q_{H_2} t_{H_2})$ 内以 $\varepsilon' \ge (\varepsilon - \frac{1}{2^k})(\frac{q_E}{q_{H_1}})^{q_E + q'_E + q_s}(\frac{q_{H_1} - q_E}{q_{H_1}})$ 优势解决 $q_E - CAA$ 问题。

引理 2 证明类似引理 1 的证明，限于篇幅，本文不给出证明。

引理 3 对敌手 II 类型，假定存在一个适应性选择消息和签名攻击算法 A_2 以在概率多项式时间 t 内以不可忽略的优势 ε 攻破了本方案，记 $q_{H_i}, q_E, q_{pk}, q_s$ 为 A_2 进行 $H_i(i = 1,2)$ 询问、私钥提取询问、公钥询问和签名询问的次数，t_{H_i}，t_E，t_{pk}，t_s 分别表示一次 H_i 询问、私钥提取询问、公钥询问、签名询问所需时间，则存在一个 (t', ε') 算法 C，在时间 $t' < t + (q_E t_E + q_{pk} t_{pk} + q_S t_S) + 2(q_{H_1} t_{H_1} + q_{H_2} t_{H_2})$ 内以 $\varepsilon' \ge (\varepsilon - \frac{1}{2^k})(1 - \frac{1}{q_{H_1}})^{q_E + q_s}\frac{1}{q_{H_1}}$ 的优势解决 $Inv - CDH$ 问题。

证明 定给 C 一个问题的实例：给定 $P \in G_1, h^* \in Z_q^*$ 和 $(r + h^*)P \in G_1$（$r \in Z_q^*$ 是未知的），C 的目标是通过与 A_2 交互输出 $\frac{P}{(r + h^*)}$。

C 运行 KGC_A 系统建立算法,挑选 $x_A \in Z_q^*$ 作为 KGC_A 系统主密钥,计算 $y_A = x_A P$ 作为 KGC_A 系统的公钥(这里 x_A 对 C 是已知的)。

C 运行 KGC_B 系统建立算法，选择 $x_B \in Z_q^*$ 作为 KGC_B 系统主密钥，计算 $y_B = x_B P$ 作为 KGC_B 系统的公钥，计算 $T = x_B y_A = x_A x_B P$ 作为系统联合公钥，并令 $X = rP$，（这里 x_B 对 C 和 A_2 是已知的，r 对 C 是未知的），C 挑选身份 ID_I 作为挑战身份，发送系统联合参数 $params = \{P, H_1, H_2, y_A, y_B, T\}$，$KGC_A$ 系统主密钥 x_A 和 KGC_B 系统主密钥 x_B 给 A_2。然后攻击算法 A_2 向挑战者 C 适应性执行下面询问：

a) H_1 询问。C 维护一个列表 H_1^{list}，该列表由表项 (ID_i,Q_i) 组成。当 A_2 进行关于身份 ID_i 的 H_1 询问时，如果该询问值已在列表中，C 返回列表中对应的值。否则 C 执行如下操作：

(a)如果 $ID_i=ID_I$，C 挑选一个随机数 $Q^*\notin\{Q_1,Q_2,\cdots,Q_{q_E}\}$ 并返回给 A_2，并增加记录 (ID_i,Q^*) 到列表 H_1^{list}。

(b)否则，C 从集合 $\{Q_1,Q_2,\cdots,Q_{q_E}\}$ 中随机挑选一个值 Q_i，并定义 $H_1(ID_i)=Q_i$，返回 Q_i 给 A_2。C 增加记录 (ID_i,Q_i) 到列表 H_1^{list}。

b)公钥询问。C 维护一个列表 pk^{list}，该列表由表项 (ID_i,Q_i,pk_{ID_i},r_i) 组成，该表初始化为空。当 A_2 进行关于 ID_i 的公钥询问时，C 检查列表中是否存在对应的值。如果存在，则输出对应的值，否则，C 从 H_1^{list} 提取出记录 (ID_i,Q_i)，然后执行如下操作：

(a)如果 $ID_i=ID_I$，令 $pk_{ID_i}=(x_Ax_B+x_AQ_i+x_BQ_i+Q_i^2)X$，返回 pk_{ID_i} 给 A_2，并且增加记录 (ID_i,Q_i,pk_{ID_i}) 到列表 pk^{list}。

(b)否则，挑选一个随机数 $r_i\in Z_q^*$，计算 $pk_{ID_i}=r_i(T+Q_iy_A+Q_iy_B+Q_i^2P)$，返回公钥 pk_{ID_i} 给 A_2。然后增加记录 (ID_i,Q_i,pk_{ID_i},r_i) 到列表 pk^{list}。

c)私钥提取询问。当 A_2 进行关于 ID_i 的私钥询问时，C 执行如下操作：

(a)如果 $ID_i=ID_I$，C 停止协议并输出“FAILURE”(该情况用 E_1 表示)。

(b)否则，C 从 H_1^{list}，pk^{list} 中提取相应的记录 (ID_i,Q_i) 和记录 (ID_i,Q_i,pk_{ID_i},r_i)，C 令 $sk_{ID_i}=(\frac{P}{(x_A+Q_i)(x_B+Q_i)},r_i)$ 并发送给 A_2。

d) H_2 询问。C 维护一个列表 H_2^{list}，该列表由表项 $(ID_i,m_i,Q_i,pk_{ID_i},h_i)$ 组成。当 A_2 进行关于 (ID_i,m_i) 的 H_2 询问时，C 随机选择 $h_j\in Z_q^*$，令 $h_i=H_2(m_i,pk_{ID_i})$。然后增加记录 $(ID_i,m_i,Q_i,pk_{ID_i},h_i)$ 到 H_2^{list}。

e)签名询问。当 A_2 进行关于 (ID_i,m_i) 的签名询问，C 执行如下操作：

(a)如果 $ID_i=ID_I$，则停止协议，输出“FAILURE”(该情况用 E_2 表示)。

(b)否则，C 从 pk^{list} 中恢复 (ID_i,Q_i,pk_{ID_i},r_i)，从列表 H_2^{list} 调出 $(ID_i,m_i,Q_i,pk_{ID_i},h_i)$，计算 $S_i=\frac{1}{r_i+h_i}d_{ID_i}=\frac{P}{(r_i+h_i)(x_A+Q_i)(x_B+Q_i)}$，C 输出签名 S_i。

最后，A_2 停止询问并输出一个挑战身份 ID^* 的消息/签名对 (m^*,S^*)，ID^* 对应的公钥为 pk_{ID^*}，且满足等式 $Verify(m^*,ID^*,pk_{ID^*},S^*)=1$，然后 C 执行如下操作：

(a)如果 $ID^*\neq ID_I$，C 输出“FAILURE”并停止该协议(该事件用 E_3 表示)。

(b)否则，C 从列表 pk^{list} 中提取相应的记录 (ID^*,Q^*,pk_{ID^*})，从列表 H_2^{list} 中提取记录 $(ID^*,m^*,Q^*,pk_{ID^*},h^*)$，从而有下面的等式成立：

$$e(S^*,h^*(T+Q^*y_A+Q^*y_B+Q^{*2}P)+pk_{ID^*})=e(P,P)$$

即
$$\begin{aligned}&e(S^*,(h^*+r)(T+Q^*y_A+Q^*y_B+Q^{*2}P)\\&=e(S^*(h^*+r)(x_A+Q^*)(x_B+Q^*),P)\\&=e(P,P)\end{aligned}$$

所以 C 可以成功地计算出 $\frac{1}{(r+h^*)}P=(x_A+Q^*)(x_B+Q^*)S^*$。C 输出数组 $\frac{1}{(r+h^*)}P$ 作为对 A_2 的挑战的应答。从而 C 解决了 $Inv-CDH$ 问题。

下面分析 C 在这个游戏中获胜的优势：

a)对 A_2 的 H_1 和 H_2 的询问的应答是均匀分布，与现实不可区分。

b)对私钥提取询问和签名预言机询问能够顺利的进行不停止，即事件 E_1，E_2 都不发生。

c)所以整体来说，如果事件 E_1，E_2 和 E_3 都不发生时，则 C 能解决 $Inv-CDH$ 问题的一个实例。则可得事件 E_1，E_2 和 E_3 都不发生的概率满足：

$$\Pr(\neg E_1\wedge\neg E_2\wedge\neg E_3)\geq(1-\frac{1}{q_{H_1}})^{q_E+q_s}\frac{1}{q_{H_1}}$$

当 A_2 没有询问 H_2 而伪造了一个有效的签名时，这种模拟是存在漏洞的，考虑到预言机输出满足均匀分布，该事件发生的概率为 $\frac{1}{2^k}$，所以 C 在该游戏中的优势为 $\varepsilon'\geq(\varepsilon-\frac{1}{2^k})(1-\frac{1}{q_{H_1}})^{q_E+q_s}\frac{1}{q_{H_1}}$，运行时间为 $t'<t+(q_Et_E+q_{pk}t_{pk}+q_St_S)+2(q_{H_1}t_{H_1}+q_{H_2}t_{H_2})$。

2.3 方案性能分析

如表 1 所示，将本文方案与近几年的椭圆曲线版本的无证书数字签名方案从签名过程，验证过程，签名长度等性能方面进行比较，其中 *Sm* 表示一次在 G_1 上的倍点运算，*Pr* 表示一次双线性对运算，*H* 表示一次映射到点的哈希运算。Tso[16]方案在签名过程中用了一次 G_1 上的倍点运算，一次映射到点的哈希运算，在验证过程用了 2 次双线性对运算，一次 G_1 上的倍点运算和一次映射到点的哈希运算。Chen[17]方案在签名过程中用了一次 G_1 上的倍点运算，在验证过程用了二次双线性对运算，一次 G_1 上的倍点运算和一次映射到点的哈希运算。Gayathri[18]方案在签名过程中用了 3 次 G_1 上的倍点运算，在验证过程用了 2 次双线性对运算，一次 G_1 上的倍点运算。Karati[19] 方案在签名过程中用了 2 次 G_1 上的倍点运算，在验证过程用了 1 次双线性对运算，2 次 G_1 上的倍点运算。相比以上的方案，本文的方案在签名过程中用了 1 次 G_1 上的倍点运算，在验证过程用了 1 次双线性对运算，1 次 G_1 上的倍点运算，结果表明本方案效率更高。在签名长度方面，比较的无证书数字签名方案中，除 Gayathri 和 Karati 签名长度为 $2|G_1|$，剩余方案都为 $|G_1|$，通过以上对比表明本方案的签名长度较短，具有较低的计算量和较高的运行效率。

表 1　方案性能比较

Table 1　Performance comparison of schemes

方案	签名过程	验证过程	签名长度
文献[16]	1Sm+1H	2Pr+1Sm+1H	|G1|
文献[17]	1Sm	2Pr+1Sm+1H	|G1|
文献[18]	3Sm	2Pr+1Sm	2|G1|
文献[19]	2Sm	1Pr+2Sm	2|G1|
本文方案	1Sm	1Pr+1Sm	|G1|

2.4 实验与仿真

在 Windows 7 操作系统下，利用微软 Visual Studio 2012 平台，结合 C 语言环境下椭圆曲线上的双线性对运算和 PBC 库实现了本文方案，然后在同一环境下(操作系统：Windows 7 64 位操作系统，CPU： Intel(R) Core(TM) i3-4150 CPU @ 3.50 GHz，内存：金士顿 HX424C15FB2 8 GB)，运行近几年的椭圆曲线版本的无证书数字签名方案，取方案运行 100 次的平均耗时进行比较，实验结果如表 2 所示，本文方案平均总耗时为 0.126s，其中签名平均耗时为 0.024s，验证平均耗时为 0.032s。本文方案平均总耗时比 Tso 方案减少了约 27%，比

Chen 方案减少了约 19%，比 Gayathri 方案减少了约 25%，比 Karati 方案减少了约 21%。

表 2 方案运行 100 次平均耗时比较

Table 2 Comparison of the average time-consuming of the 100 results

方案	签名平均耗时/s	验证平均耗时/s	方案平均总耗时/s
文献[16]	0.031	0.071	0.173
文献[17]	0.028	0.046	0.155
文献[18]	0.083	0.041	0.167
文献[19]	0.059	0.037	0.159
本文方案	0.024	0.032	0.126

3 结束语

本文在现有的无证书密码体制的基础上，提出了一种基于双重 KGC 的无证书短签名方案，并且在随机预言机模型下，证明了本文方案在适应性选择消息攻击下是存在性不可伪造的。本文方案的双重 *KGC* 之间相互制约，具有分权的效果，从而降低了 *KGC* 主密钥泄露的概率，减少了因为 *KGC* 主密钥泄露和 *KGC* 被恶意用户操控对系统产生的危害，提高了方案的安全性，并且方案的签名长度较短，若 G_1 为 160 比特的椭圆曲线群，则本文的签名长度只有 160 比特。综上知，本文方案具有运行效率较高，计算量较低，签名长度较短，实用性和安全性较强等特点，适用于宽带较低的环境中，并且双重 *KGC* 的特性更易于 *KGC* 的部署和云化 *KGC* 的实现。在实际应用中，对于身份认证而言，光依靠签名是不够的，还需要结合其他技术比如双因子认证[20,21]来加强安全性，因此进一步的研究重点是如何在应用开发中实现多种技术融合身份认证。

参考文献：

[1] Shamir A. Identity-based cryptosystems and signature schemes [C]//Proc of Workshop on the Theory & Application of Cryptographic Techniques.Berlin:Springer,1984: 47-53.

[2] Alriyami S S, Paterson K G. Certificateless public key cryptography [J]. Asiacrypt, 2003, 2894(2): 452-473.

[3] 冯蕾，彭长根，彭延国. 一种高效的无证书多重签名方案[J].计算机应用研究，2012, 29(2): 644-645. (Feng Lei, Peng Changgen, Peng Yanguo. Efficient certificateless multi-signature scheme [J]. Application Research of Computers, 2012, 29(2): 644-645.)

[4] Islam S H, Obaidat M S. Design of provably secure and efficient certificateless blind signature scheme using bilinear pairing [J]. Security & Communication Networks, 2016, 8(18): 4319-4332.

[5] Gao Zhuo, Hu Liang, Li Hongtu. A new efficient leakage-free certificateless signature [C]//Proc of International Forum on Mechanical, Control and Automation. Paris: Atlantis Press, 2017: 978-986.

[6] Gong Zheng, Long Yu, Hong Xuan, *et al.* Two certificateless aggregate signatures from bilinear maps [J]. Journal of Information Science & Engineering, 2007, 26(6): 2093-2106.

[7] 张永洁，张玉磊，王彩芬. 聚合签名方案的安全性分析与改进 [J]. 计算机应用与软件，2017, 34(8): 307-311. (Zhang Yongjie, Zhang Yulei, Wang Caifen. Security analysis and improvement of aggregate signature schemes [J]. Computer Applications and Software, 2017, 34(8): 307-311.)

[8] Chen Yuchi, Horng G, Liu Chaoliang. Efficient certificateless aggregate signature scheme [J]. Journal of Electronic Science and Technology, 2012, 10(3): 209-214.

[9] 喻琇瑛，何大可. 一种新的无证书聚合签名 [J]. 计算机应用研究，2014, 31(8): 2485-24879. (Yu XiuYing, He Dake. New certificateless aggregate signature schemes [J]. Application Research of Computers, 2014, 31 (8): 2485-24879.)

[10] 张玉磊，周冬瑞，李臣意，等. 高效的无证书广义指定验证者聚合签名方案 [J]. 通信学报，2015, 36(2): 48-55. (Zhang Yulei, Zhou Dongrui, Li Chenyi, *et al.* Certificateless-based efficient aggregate signature scheme with universal designated verifier [J]. Journal on Communications, 2015, 36(2): 48-55.)

[11] 葛丽霞，李嫀，何明星，等. 一个改进的无证书代理签名方案 [J]. 计算机工程与应用，2017, 53(8): 92-94. (Ge Lixia, Li Xiao, He Mingxing, *et al.* Improved certificateless proxy signature scheme [J]. Computer Engineering and Applications, 2017, 53(8): 92-94.)

[12] 刘晓红，张建中. 对一种无证书代理签名方案的分析与改进 [J]. 计算机工程与应用，2014, 50(22): 115-117. (Liu Xiaohong, Zhang Jianzhong. Analysis and improvement of certificateless proxy signature scheme [J]. Computer Engineering and Applications, 2014, 50(22): 115-117.)

[13] Boneh D, Lynn B, Shacham H. Short signatures from the weil pairing [C]//Proc of the 7th International Conference on the Theory and Application of Cryptology and Information Security. Berlin: Springer, 2001: 514-532.

[14] Boneh D, Franklin M. Identity-based encryption from the weil pairing [J]. Siam Journal on Computing, 2003, 32(3): 213-229.

[15] Galbraith S, Harrison K, Soldera D. Implementing the tate pairing [C]// Proc of International Symposium on Algorithmic Number Theory. Berlin: Springer, 2002: 324-337.

[16] Tso R, Huang Xinyi, Susilo W. Strongly secure certificateless short signatures [J]. Journal of Systems & Software, 2012, 85(6): 1409-1417.

[17] Chen Yuchi, Horng G, Liu Chaoliang. Strong non-repudiation based on certificateless short signatures [J]. Iet Information Security, 2013, 7(3): 253-263.

[18] Gayathri N B, Reddy P V. Efficient certificateless signature scheme with provable security [C]//Proc of IEEE International Conference on Advanced Computing. 2016: 322-337.

[19] Karati A, Islam S H, Karuppiah M. Provably secure and lightweight certificateless signature scheme for IIoT environments [J]. IEEE Transactions on Industrial Informatics, 2018, 14 (8): 3701-3711.

[20] He Debiao, Wang Ding. Robust biometrics-based authentication scheme for multiserver environment [J]. IEEE Systems Journal, 2015, 9(3): 816-823.

[21] Wang Ding, Wang Ping. Two birds with one stone: two-factor authentication with security beyond conventional bound [J]. IEEE Trans on Dependable and Secure Computing, 2016, 15(4): 708-722.